SDWANの設定グループを使用したセキュリティ機能の有効化

内容

はじめに

このドキュメントでは、統合ロギングの手順を含め、NGFW、URLフィルタリング、AMP、およびIPS/IDSを設定グループ経由で設定する方法について説明します。

前提条件

フローの可視化とアプリケーションの可視化を実現

ポリシーグループを使用してポリシーを定義している場合（デフォルト）。

- Policy groupを選択してから、Application priorityとSLAを選択します。
- [新規追加（Add New）] を選択します。
- Additional settingsをクリックし、Application visibilityとFlow visibilityを有効にします

レガシー・ポリシーを使用している場合

- Configuration GroupでCLIアドオンプロファイルを選択し、次のコマンドを追加します

```
policy
app-visibility
flow-visibility
```

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/url-filtering.htmlで説明されている機能の前提条件を満たしていることを確認します。

```
Note: If you are using the legacy policy along with Configuration groups :

Select Configuration and Click Security
Click Custom Options and select Policies/Profiles and then access these features to enable
```

このドキュメントでは、ポリシーグループを使用して有効にする機能に焦点を当てています

次世代ファイアウォール(NGFW)

NGFWを有効にするには、次の手順を実行します。

- Policy groupを選択し、NGFWをクリックしてからAdd NGFW Policyをクリックします
- ポリシー名を指定して、Nextをクリックします
- NGFWポリシーに関連付ける設定グループの選択
- ルールを追加し、[次へ]をクリックします
- NGFWポリシーの作成

ロギングを有効にするには、NGFWポリシーを編集してから追加設定を選択し、統合ロギングをオンにします

URL フィルタリング

20.18より前のリリースでURLフィルタリングを有効にするには、次のコマンドを実行します。

- UIでConfiguration、Policy groupの順に選択し、Groups of Interestをクリックします
- Securityを選択してからProfilesを展開します

リリース20.18以降でURLフィルタリングを有効にするには、次のコマンドを実行します。

- UIの設定、ポリシーグループの順に選択し、次にObjects and Profilesをクリックします

- セキュリティプロファイルの選択

Add url filteringを選択し、詳細を入力してsaveをクリックします

Advanced Malware Protection（AMP）

20.18より前のリリースでAMPを有効にするには：

- UIでConfiguration、Policy groupの順に選択し、Groups of Interestをクリックします
- Securityを選択してからProfilesを展開します

リリース20.18以降でAMPを有効にするには、次の手順を実行します。

- UIの設定、ポリシーグループの順に選択し、次にObjects and Profilesをクリックします
- セキュリティプロファイルの選択

Advanced Malware Protectionを選択し、Add Advanced Malware Protectionをクリックします

詳細を追加し、[保存]をクリックします

侵入防御システム(IPS)/侵入防御検出(IDS)

20.18より前のリリースでIPS/IDSを有効にするには、次のコマンドを実行します。

- UIでConfiguration、Policy groupの順に選択し、Groups of Interestをクリックします
- Securityを選択してからProfilesを展開します

リリース20.18以降でIPS/IDSを有効にするには、次のコマンドを実行します。

- UIの設定、ポリシーグループの順に選択し、次にObjects and Profilesをクリックします
- セキュリティプロファイルの選択

Intrusion Preventionを選択し、Add Intrusion Preventionをクリックする

詳細を追加し、[保存]をクリックします

拡張検査プロファイル(AIP)の作成

20.18より前のリリースでAIPを有効にするには、次のコマンドを実行します。

- UIでConfiguration、Policy groupの順に選択し、Groups of Interestをクリックします
- Securityを選択してからProfilesを展開します

リリース20.18以降でAIPを有効にするには、次の手順を実行します。

- UIの設定、ポリシーグループの順に選択し、次にObjects and Profilesをクリックします
- セキュリティプロファイルの選択

「拡張検査プロファイル」を選択し、「拡張検査プロファイルの追加」をクリックします

- 前の手順で作成したAMP/IPS/URLフィルタリング名を入力し、saveをクリックします

NGFWへのAIPの関連付け

- Configurationを選択してからPolicy groupsを選択し、NGFWをクリックします
- 前に作成したNGFWポリシーを編集します。
- 先に作成したNGFWルールについて、先に作成したAIPプロファイルを編集して関連付け、保存をクリックします

Ulogging

ロギングを行うには、cli add onを使用して設定グループ経由でルータ上の機能を有効にします。

```
policy
ip visibility features
ulogging enable

parameter-map type inspect-global
log dropped-packets
log flow-export fnf
log flow
!
utd engine standard unified-policy
utd global
flow-logging all
```

検証

```
show  flow monitor sdwan-flow-monitor cache

IPV4 SOURCE ADDRESS:                            10.100.10.75
IPV4 DESTINATION ADDRESS:                       10.10.10.25
TRNS SOURCE PORT:                               53
TRNS DESTINATION PORT:                          34796
IP VPN ID:                                      10
IP PROTOCOL:                                    17
tcp flags:                                      0x00
interface input:                                Gi2
interface output:                               Gi3
flow cts source group tag:                      0
flow cts destination group tag:                 0
counter bytes long:                             125
counter packets long:                           1
timestamp abs first:                            14:59:47.613
timestamp abs last:                             14:59:47.613
flow end reason:                                Not determined
connection initiator:                           Reverse initiator
interface overlay session id input:             10
interface overlay session id output:            0
connection connection id long:                  0x000000000050D9CC
drop cause id:                                  0
counter bytes drop long:                        0
sdwan sla not met :                             0
sdwan preferred color not met :                 0
sdwan queue id :                                2
counter packets drop long:                      0
ulogging fw zp id:                              4
ulogging fw zone id array:                      3 3
ulogging fw class id:                           12544961
ulogging fw policy id:                          5559936
ulogging fw proto id:                           25
ulogging fw action:                             2
ulogging fw drop reason id:                     0
ulogging fw source ipv4 address translated:     0.0.0.0
ulogging fw destination ipv4 address translated:  0.0.0.0
ulogging fw source port translated:             0
ulogging fw destination port translated:        0
ulogging utd ips pri:                           1
ulogging utd ips sid:                           57756
ulogging utd ips gid:                           1
ulogging utd ips cid:                           21
ulogging utd urlf url hash:                     00000000000000000000000000000000
ulogging utd urlf url category:                 0
ulogging utd urlf url reputation:               0
ulogging utd urlf application name:
ulogging utd amp dispos:                        0
ulogging utd amp filename hash:                 00000000000000000000000000000000
ulogging utd amp file type:                     0
ulogging utd amp file hash:                     0000000000000000000000000000000000000000000000000000000000000000
ulogging utd amp malname hash:                  00000000000000000000000000000000
ulogging utd drop reason id:                    0
ulogging sdvt drop reason id:                   0
ulogging utd ips policy id:                     1
ulogging utd ips action id:                     1
```

```
ulogging utd urlf policy id:                        N/A
ulogging utd urlf action id:                        N/A
ulogging utd amp policy id:                         N/A
ulogging utd amp action id:                         N/A
ulogging utd urlf reason id:                        0
ulogging ulogging flow direction:                   Reverse initiator
ulogging fw user name:
ulogging fw source ipv6 address translated:         ::
ulogging fw destination ipv6 address translated:    ::
ip dscp:                                            0x00
application name:                                   port dns
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。